A Vision of the Internet of Things: A Review of Critical Challenges

Zahra Valadkhani
Department of Electrical and Computer Engineering,
Faculty of Shariaty, Tehran Branch, Technical and
Vocational University(TVU), Tehran, Iran.
Email: bahare.valadkhani [AT] gmail.com

Branka Rodić*
Academy for Applied Studies Belgrade, College of
Health Sciences, Belgrade, Serbia.
Email: brodic [AT] gmail.com

Farhad Lotfi
Young Researchers and Elite Club, South Tehran
Branch, Islamic Azad University, Tehran, Iran.
Email: st_f_lotfi [AT] azad.ac.ir

Abstract—**Today, Information Communication Technology has brought many benefits to have a better life. Meanwhile, the concept of the Internet of Things (IoT), which has transformed the traditional lifestyle into a modern lifestyle and is growing rapidly, is of great importance. This research deals with the critical challenges of IoT. Although not much time has passed since the advent of the concept of the IoT, today the Internet of Things has faced a great deal of complexity in the industry, which requires in-depth studies to realise its potential and challenges. This study introduces and examines IoT challenges including security and privacy, scalability, interoperability, mobility, protocol & standardisation, and energy consumption. In this study, the relationship between these challenges has been clearly defined. Finally, based on the research, some main challenges or sub-challenges considered for these challenges.**

Keywords-component: The Internet of Things, Challenges.

I. INTRODUCTION

In the 21st century, considering the population growth in metropolitan areas and its complexities, the Internet of Things (IoT) is of particular importance. [1] has pointed out that smart city is strongly based on information and communications technology. Thus, it is clear that IoT plays a key role in shaping and maintaining smart city puzzles including smart education, smart security, smart health, smart transportation, smart home, and so on.

Because not much time has passed the advent of IoT, it defines as the connection and integration of all devices connected to the Internet. It is noteworthy that the connection of these devices with other devices, communication and connection of the device with objects in the environment, connection of objects and some devices with humans are managed through the web space [2]. Moreover, the principle is to offer and exchange information in real-time, on the other hand, related software and applications should seem so user-friendly.

It can be claimed that the basic idea of IoT relates to the study “the 'only' coke machine on the internet” (Department of Computer Science, Carnegie Mellon University - 1982), this study describes how the first device to connect to the Internet. Later in 1992, a new structure called RPC was defined at Cambridge University, in which a network with the ability to provide multiple services was able to connect the Trojan room to the Internet. Since then, researchers have conducted more studies in this area. Investigations continued until Ashton (1999) succeeded in establishing real-time communication between objects. Schoenberg was eventually one of the first to use the term “IoT”. Waldo describes IoT as follows: The Internet of Things is similar to the state in which humans are an integral part of the Internet and those who perform the calculations are the real beneficiaries. It was at this time that objects gained digital identity and the possibility of organising and managing them in the world of the Internet became possible [3].

Clearly, it can be said that IoT is responsible for connecting and computing objects, humans, electronic devices such as cameras, sensors, computers, smart mobile phones, wearable, and similar devices.

According to [4] there are several important the Internet of Things features that should be considered:

- Identification: Here means that all objects must be recognisable. If there were objects that were unique, the problem could be solved by labelling with RFID or QR and such tools. In this way, identification can easily be done by an authentication device. There is another way to fix this node, the object can be provided with its information.
- Reception: Objects can be connected to the physical environment anonymously (i.e., receiving operations), or explicitly (i.e., performing actions).
- Other features of IoT include the connection between everything, the identification of everything, as well as the interaction between everything [4].

Generally, smart objects can communicate with themselves or their surroundings through communication channels, where each object can be identified. IoT makes it possible for calculations of all objects to be present at any place or time.

Figure 1 explains the features of the main the Internet of Things system levels:

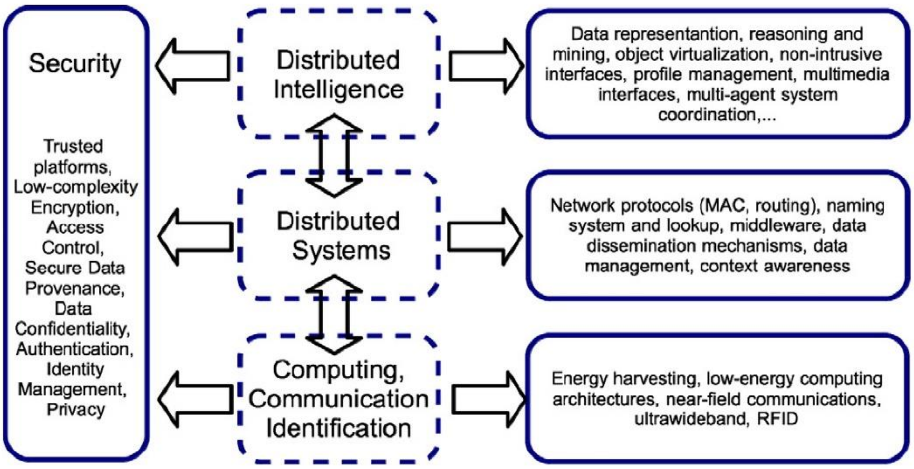
Security
Trusted platforms, Low-complexity Encryption, Access Control, Secure Data Provenance, Data Confidentiality, Authentication, Identity Management, Privacy
Distributed Intelligence
Distributed Systems
Computing, Communication Identification
Data representantion, reasoning and mining, object virtualization, non-intrusive interfaces, profile management, multimedia interfaces, multi-agent system coordination,...
Network protocols (MAC, routing), naming system and lookup, middleware, data dissemination mechanisms, data management, context awareness
Energy harvesting, low-energy computing architectures, near-field communications, ultrawideband, RFID

Fig.1. Classification of the Internet of Things related research areas [4].

- Computing, communication and identification technologies: Regarding computing, communication and identification technologies, the realisation of IoT scenarios, there should be comprehensive development of advanced techniques that are able to identify and understand capabilities such as computing, communication and identification in daily objects.
- Distributed Systems Technology: This span includes a definition of all aspects of IoT to create a distributed network that provides services in a better condition and quality [5]. It can be concluded that the ability to recognise different objects in distributed systems increases, on the other hand, it should not be forgotten that there are many problems and obstacles in the path of growth and development.
- Distributed Intelligence: Although there is smart communication in an IoT system, there is a need for more accurate communication coordination and computation for better planning. In the IoT, big data is an issue because smart devices pass a lot of data at any given time. IoT has provided solutions to this data, such as data mining and its evaluation, as well as a knowledge management system that ultimately leads to satisfaction [4]. In fact, if a task is considered very simple, it still requires coordination from various parts. Genuinely, IoT is the design of programmes in which control is based on a single factor.
- Security: In fact, it is the security that increases the acceptance of technology by users and it is a key issue in IoT. Critical issues such as privacy play an important role in increasing the security factor and acceptance of new technology by users [4].

Thus, it should be noted that this research believes that although users are looking for high speed in IT applications, it is obvious that high speed sometimes poses security threats. In the following, some of these challenges and threats are discussed.

Over time, the world population is growing increasingly. The United Nations Population Fund (UNFPA) has released a report on population growth, which predicts that the population over the age of 60 will increase to 2 billion by 2050. In addition, another report prepared and published by the World Health Organisation (WHO) in 2013, which estimated that there was a shortage of nearly 7.2 million people in the field of health care, which was expected to reach 12.9 million by 2035 [6]. In recent years, IoT has taken very effective steps in various fields, such as in the health sector [7].

The benefits of using the Internet of Things knowledge in the present century in both industrial and scientific environments recognised [8].

Today, the infrastructure of developed cities relies on the knowledge of ICT. Stakeholders offer solutions to make IoT meet real-time responsiveness. Of course, it should be noted that standardisation of remote services is developing [9].

Thus, this research believes that due to population growth as well as the ageing population that is ahead, now it is not possible to send, receive or manage data in the traditional context [6]. Here, the advent of the Internet of Things comes into play in various service areas, and given its scale and the emergence of new challenges, it provides a platform for research and new solutions.

Therefore, one of the main concerns of this study is to examine some key and challenging factors in the field of IoT. This article also faced limitations such as the lack of an integrated IoT system. However, the main and important approach of this study is to examine 6 existing IoT challenges. These challenges include security and privacy, scalability, interoperability, mobility, protocol, standardisation, and energy consumption.

According to studies, these 6 factors are important challenges in the Internet of Things. In the research methodology section, for each main challenge, sub-factors or features are also considered and content is also presented. In this study, 315 articles and findings of researchers were reviewed and finally 155 of them used in this study. They were omitted mainly due to their heterogeneity and inconsistency with this research.

These papers were mainly extracted and reviewed from databases such as Elsevier, Springer, IEEE Explore, Google Scholar, and Research Gate in the field of IoT challenges. The study began in July 2020 and was completed in early December 2020. In the literature review section, there are points to what researchers have pointed out in this regard and what they have not pointed out in this regard.

After the introduction, a review of the related literature has been prepared. In the third part, the research methodology is given. Finally, conclusion is presented.

II. LITERATURE REVIEW

A. An overview of the Internet of Things concepts and new achievements in this field

IoT is an interdisciplinary debate that is evolving in industry and academia in parallel. Although not much time has passed since the advent of this technology, it has been able to bring valuable services to people and have a significant impact on the growth of individuals' capabilities [10].

Hence, IoT has affected user behaviour today. Its flexibility and integration have been able to increase communication and individuals' satisfaction. Given the presence and extent of IoT in various industries, the today's modern world is witnessing dramatic changes. Today, a major part of business has been changed from traditional to electronic, and progress in this area can be felt instantly [11].

The other article [12] argued that IoT has a high degree of flexibility in complex systems and has also accelerated detection. They then examined the routing data as well as the amount of data generated by the sensor on the structures. They added that the sensing system is expanding using RFID in wireless communications as a monitoring knowledge. Furthermore, IoT has a set of protocols in which objects transmit data by sensors and cameras, each of which has a unique identity.

IoT does not end here; it is connected to a vast science. For instance, in software production, many different aspects must be considered so that there is no problem in maintaining IoT systems. A recent study by [13] a survey of 53 countries was conducted, considering the characteristics of IoT systems, concluded that the field need human intervention currently since advanced learning systems are still in their growing steps and have not received the necessary adaptation from the environment.

Several researches focused on COVID-19 diagnosis based on real extracted patients' data. After developing a model, the conducted experiment tried to diagnose disease by eight machine learning algorithm. Among them, five algorithms showed more than 90% detection accuracy [14]. Many studies today target and focus on "real-time" responsiveness. As noted in [15], real-time responsiveness increases user satisfaction and this makes systems and projects sustainable in the field of IoT.

It should be noted that the presence of the Internet of Things in different areas of the smart city is normal and mandatory. The spread and use of IoT in various industries and scientific environments have faced various complexities and challenges. To address such challenges, new standards are needed. For example, [16] introduced a framework. According to ISO and ICE standards, they presented a comprehensive model called DFR, which addresses some of the shortcomings in the field of digital forensics.

Finally, it should be added that there are few places where IoT has not stepped. It is possible that the scope of this field is increasing day by day, which on the other hand also it involves various sciences. The next section provides background information on the challenges of IoT.

B. An Overview of 6 Critical Challenges in IoT

Security and Privacy: It is not easy to say that the arisen problems and challenges are related to which institution or organisation and which authority should take care of them. This study believes that both industry and academia should share their theoretical and practical experiences at every level to address the challenges of the Internet of Things. In this case, the effective and efficient steps of IoT can be considered. There are some anomalies in the diagnosis of some problems in the field of IoT. [17] addresses these challenges, which include error detection, communication networks, issues and challenges in social networks, and, of course, security and privacy.

The most recent [18] achieved the desired results. They introduced a security mechanism called IoT-NetSec. This mechanism prevented some possible attacks that might occur in the service.

In IoT macro issues, security has sometimes been considered in terms of privacy, and this study also examined the security factor with privacy in one factor. According to [15] stated that privacy is a principle for the successful maintenance of the Internet of Things projects. They added that at the beginning of any project regarding IoT, user privacy should be considered first and end-users should be fully assured about respecting and maintaining the privacy of their information. If individuals are confident in their information privacy and are aware that their information will be stored in a secure environment, they will express their satisfaction with the new services and technologies and loyalty to such services will be established.

In the context of IoT, it must be ensured that the data exchanged is visible only to the sender and receiver. On the other hand, [16] conducted research on IoT security factor and its challenges. They considered the control of IoT access and tracking of messages sent or received as very important.

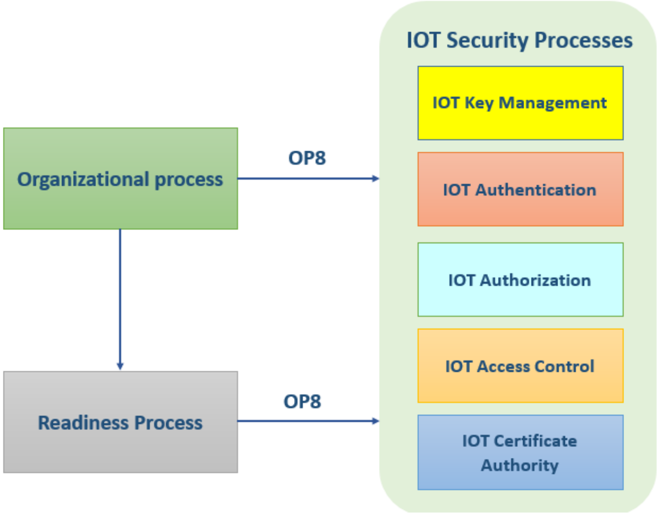

Fig.2. Security factor processing in the Internet of Things [16].

Figure 2 shows the processing of security in IoT so that after organisational processing, authentication operations are considered and access is possible after authentication. Generally, in this type of control, access is ensured from tracking and all sending and receiving, and this type of service can be monitored. Finally, it should be noted that the diversity of the Internet of Things system determines the extent of security and other challenges.

Scalability**:** The next factor that is examined in this article is scalability. Generally, scalability in IoT context means the ability of a system to manage, as well as the potential of this system for small and large tasks. [19] focused on scalability in their research. They acknowledged that in order to have high scalability, an advanced security system is also necessary in a system. Furthermore, if the intelligence of objects goes upwards, the management of this scalability becomes more effective and efficient. In the meantime, one of the important tasks of IPv6 is to monitor the scalability of the network.
However, the study [17] has identified scalability as one of the key challenges in the Internet of Things. Also, tried to model IoT in the context of a social network to solve scalability problems. They also used the cloud for progress and productivity, and finally added that accuracy also increases the scalability of relationships and interactions between objects and humans [17].
In addition to these reasons, [20] argued that many IoT puzzles are interrelated and in order to have a useful and advanced authentication system, one must pay more attention to the scalability factor.

Interoperability: This means the exchange of sent and received data between different devices. According to IoT studies, interoperability can be considered as one of the primary methods for the IoT framework [21]. Therefore, [22] also emphasised the importance of interoperability in the Internet of Things. They added that interoperability is very important since in integrating devices, different operating systems must be supported and a reliable environment must be provided. Many articles have discussed the interoperability factor and many management approaches have been adopted as solutions for interoperability. [23] considered interoperability to be mandatory for network standards implementation. According to [25] on interoperability, information from different companies, industries, or regions will be exchanged. Then, [25] considered the use of interoperability in the network and in the physical layer as of great importance. However, the growth and sustainability of IoT depends on interoperability, privacy and security, as well as the energy factor. Finally, it should be added that interoperability creates a common language between all devices and smart objects so that different programmes with different times and places can interact without any problems.

Mobility: This factor is very important in smart cities and it plays a role in various smart city puzzles such as smart health, smart transportation, and smart education so on. For instance, in the city of Tampere, Finland, an application is designed so that individuals can meet each other in different places at the same place and time. This application, which is installed on smart mobile phones, is able to offer users the type of route and the type of means of transportation in proportion to vehicle traffic in the city, so that users can reach their desired location at a specific time [25]. According to [26] cited mobility as one of the key factors in the growth of wireless electronic devices. Since most individuals in the society have a computer, laptop, or tablet, it is not yet provided the standard network for communication. Mobility is one of the challenges of the Internet of Things, so one should always strive to improve it, since it plays an important role in promoting the user-friendliness of IoT-related programmes.
[27] was a review on IoT-Fog-Cloud. Also, they have studied how the Internet of Things applications are managed. This study showed that energy, computing and mobility are at heterogeneous levels. One of the ideas of the study [27] was that

in 5G network, the network can be divided into different and small parts and each part of this network can be provided for different needs such as mobility support.

Protocol & Standardisation: With the formation of the network, the concept of protocol and standardisation has always been important. In fact, a protocol is a set of standard rules and regulations that allow communication between different devices. In the study [28] made hints in this regard. According to them, in IoT services, protocols are sometimes restricted and the system architecture is responsible for linking illegal and limited protocols. This study also considers security and privacy as a single factor. In addition, standardisation and interoperability have been mentioned as other challenges in the Internet of Things. Generally, standardisation is a concept used for social and economic challenges and new business models. There are many institutions in the world that define protocols and standards in the networking world, such as The European Telecommunications Standards Institute (ETSI) in Europe and the Institute of Electrical and Electronics (IEEE) in the United States.

It should be noted that in communication, standardisation has come to the aid of interoperability criterion to eliminate heterogeneous resources [28]. [29] focuses on the challenges of IoT. They also examined the protocol factor in terms of network error and protocol security. However, due to new needs and network expansion in different contexts, new protocols need to be defined.

[30] argued that the lack of some standards and challenges in this field leads to the limitation of IoT. Some challenges raised include challenges in data management, scalability, real-time data processing, security and privacy, interoperability, and lack of standardisation. They also mentioned the ZigBee wireless protocol. ZigBee is a wireless network standard that is energy efficient. Delay in data exchange on ZigBee is very low and the international standard for it is IEEE 802.15.4. It goes without saying that IoT devices require specific practical protocols for each. According to [30], standardisation actually guarantees interoperability, and this makes sharing integrated and successful.

Energy Consumption: It is one of the most challenging issues in the technology world. Electronic devices, in addition to sometimes using a lot of energy, also heat the environment. Meanwhile, Microsoft [31] has come up with solutions. Some ideas, such as putting these electronic devices in the ocean, pose a risk to the environment that could have devastating consequences later. This study believes that technology does not always bring 100% benefit to individuals in the community and it may have disadvantages in the beginning, as the waves of smart mobile phones and satellites that cause various harms to humans. But such losses can be minimised through study, research and experimentation.

Optimal energy consumption has always been one of the most important challenges in IoT to be able to see the integration in standard communication [4].

[28] has argued that protocols that use simple routing always suffer from less computational complexity and less energy.

In addition to these reasons [32] focused deeply on the challenges of the Internet of Things. They categorised energy into technical challenges and acknowledged that energy remains one of the major challenges in the field of information technology such as systems based the ICT [33]. Also, [32] believes that current policies and programmes do not meet the needs of IoT and today’s challenges.

However, according to the studies that this article has done for privacy and security and of course other main factors (Figure 3), other challenges have been extracted in the heart of these factors, which are discussed in the next section.

It should be noted that as a result of the studies of this article, some factors have a high number of citations and vice versa. This does not mean some factors have been less studied, but rather that some IoT challenges such as privacy and security have been the most studied among articles published by different magazines and databases.

Finally, this study attempts to discuss the generalities of IoT-related topics. In addition, regarding the critical and challenging factors of the Internet of Things, this article could point out to some extent what the researchers have said and what they have not said.

III. RESEARCH METHODOLOGY

Due to the extent of the Internet of Things and its overlap with various fields, many factors are involved with the Internet of Things and it creates challenges as it develops. Each of them may play an important role in some areas and vice versa as IoT has entered various fields of health, industry, economy, business, etc. Different researchers specialise in each of the fields they enter, taking into account the challenges of that field to conduct their research and provide optimal solutions. However, some of the challenges, regardless of the field in which they operate, are general and can help individuals who study IoT to present their solutions optimally, taking into account the real challenges and open vision, or produce related products. For this reason, this study introduces general challenges related to all areas of IoT, having the most overlap in the Internet of Things. Therefore, IoT technology can claim success and epidemic if the extracted challenges are carefully examined and finally solved.

In this study, 315 scientific articles and researches were extracted from reputable scientific databases such as Elsevier, Springer, IEEE Explore, Google Scholar, and Research Gate along with several reputable scientific websites and they were reviewed. Finally, 155 scientific articles were selected and used to write this article. There were many reasons for omitting some articles that were put aside. For example, articles such as IoT Challenges in Big Data, Smart Health, Smart Sensors, Wireless Networks, Cloud Computing, and Fog Computing.

The findings and material were examined that had the most convergence.

Today, communication has a very high cost, so the steps must be done properly and with a plan so that the work can be witnessed in real-time. On the other hand, [24], the use of IoT has been evaluated very differently according to the needs of the end-user. Due to the complexity and difficulty of the task, this study attempts to examine six key and interrelated factors together. Figure 3 illustrates these key IoT challenges.

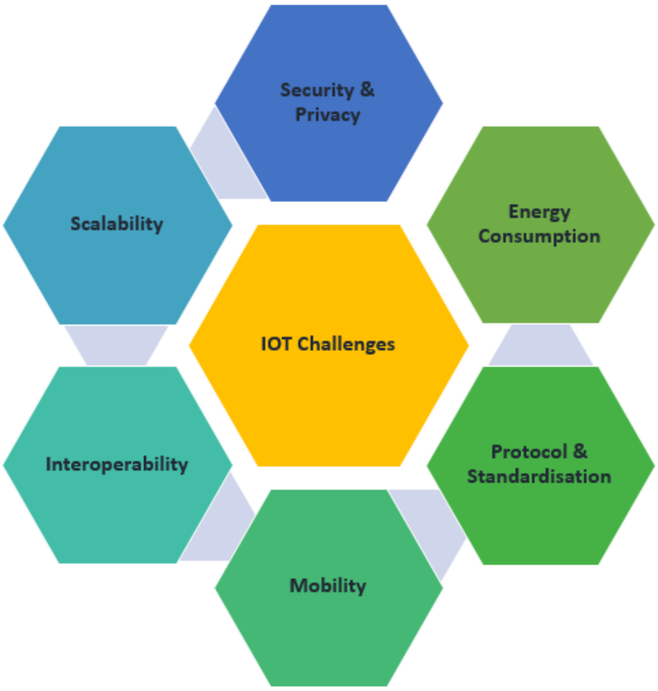

Fig.3. the Internet of Things Critical Challenges.

Security is a prerequisite for starting any IoT project or service, as stated [34] privacy must be maintained in this field by maintaining and protecting data. They added that IoT is accepted by the public when people make sure that their information is protected in this context.

It can be argued that with the advent of the Internet of Things, many of the challenges in the field of ICT became more apparent. Scholars have considered mechanisms such as encryption and authentication system for this [35]. Generally, users and end users of IoT services expect speed and of course quality. It is normal that security is seriously challenged when it comes to speed. Therefore, this study examines security and privacy at first glance. In this study, access control is the first challenge posed by security and privacy. Access control in a programme is possible when authentication is done; this is accomplished today in various ways [22].

Generally, in order to overcome a crisis and a challenge such as access control, requirements must be considered. These include requirements such as confidentiality and authentication. Access permission is issued after authentication; secure communication is achieved in such condition [26]. Then, went on to say that trust is essential to IoT. In this article, trust is under the factor of security and privacy, as well as different meanings of the concept of trust in research findings. Thus, it can be said that there is no definite opinion about trust, although this is important for the Internet of Things.

[36] have used the term trust management in their research. They mentioned trust as one of the RFID security issues and also considered it necessary to pay attention to trust management in order to improve the features of wireless sensor networks. In the continuation of the challenges included in security and privacy, two factors of identification and authentication are discussed together due to convergence [37]. On the other hand, in IoT, it is possible to identify and authenticate a unique object. For example, to identify some products, a unique QR code is used, which has made identification easier. Additionally, in the previous section, RFID radio frequency identification was mentioned [38]. Access control and authentication mechanisms are used in most IoT applications. The concept of Integrity is another method that is defined along with confidentiality and integrity. Security and its current challenges ahead do not end here and they have a broader concept.

One of the most basic concepts in the Internet of Things security is confidentiality. It depends on several factors, here data sensitivity should be measured and a protection mechanism should be considered in proportion to the level of data sensitivity [37]. Confidentiality is indeed a security and privacy challenge. Confidentiality should ensure that the information exchanged should not be understood or read by anyone. This continues until it is ensured that the end user has access to the information after authentication and identification [38]. Accessibility is actually one of the last issues in security that should be considered and is usually raised after issues such as confidentiality and integrity. After authentication and identification of the user, the data or information must be available in real-time [39].

The concept of scalability implies in different areas of management in the field of network. A scalable network solution is essential to achieve the benefits of the various IoT domains. Thus, the network can support millions of subscribers when it is scalable. The concept of scalability also reduces costs and ease of operation. Sensors, cameras, and other electronic devices in IoT require a coherent interaction. When the number of data sent and received on IoT reaches a billion objects or more, the scale and complexity also expand. This leads to scalability in network management [23].

[29] has acknowledged that scalability has features that should be considered in the implementation of IoT services. These features include software, hardware, marketing, networking, and business. This study believes that these features should be considered in many stages. For instance, marketing and market knowledge should be studied and assessed before starting any project. IoT has moved to the point where it can now turn data and information into knowledge, and the challenge of scalability is defined here. Although this article argues that some scalability features such as marketing and business should be studied before the project, some features and challenges such as software efficiency and user-friendliness are identified during the work.

Thus, [27] discussed the concept of interoperability after the scalability challenge. Interoperability makes sense in network congestion and delays in sending and receiving calculations. In this article, interoperability is a principle in IoT since it is not yet accepted in many industries and still has a lot of margins due to privacy. Due to the extent of the network and the importance of this issue, the need for valid protocols has been felt more in the world, and in the meantime, the IPv6 protocol has been introduced. [19] has raised the issue of interoperability following the advent of IPv6. In [40] IPv6 has been researched as a key strategy and feature.

According to [41], in order to achieve the ideals of interoperability, several other challenges have been defined that should be regarded. [41] considered the virtual representation of things, searching, finding and accessing thing, and syntactic interoperability between things as the key interoperability challenges. Despite advances in technology, virtual display of an object, search, find and access to an object, and interoperability are still key challenges that need a lot of work.

Another challenge that this article faced was the issue of mobility. Mobility is enabled through protocols such as IPv6. [38] has developed solutions for mobility from a management perspective. In other words, interoperability is one of the management requirements of mobility in dynamic systems, and IoT systems must have adequate monitoring and management of mobility in order to have stable security.

Network protocols and the IoT infrastructure in general must be so that they have the highest level of flexibility. Mobility is one of the issues that is very changeable and should be managed in the Internet of Things environment. Mobility variability becomes more prominent in networks such as Ad-Hoc. One of the mobility features is movement detection, which monitors devices and it is necessary to respond to changes [19].

In other words, one of the features that distinguish IoT from many other new technologies is the concept of mobility. This is very sensitive in some places such as hospitals and medical centres. [42] argued, there are two very important features in mobility that should be considered in the management debate. The first characteristic is the detection of movement of the device and the second one is control messages. According to the findings in this article, for the Internet of Things security issues, it is necessary to monitor devices and many fixed and variable objects, and on the other hand, monitor and control network traffic to optimise both management and prevent possible attacks. This issue has grown in today’s world, but some end users of new services and technologies still do not allow their location to be identified and monitored, and therefore these two features can be in the category of mobility challenges.

The next challenge discussed in this article is protocol and standardisation in one perspective and in the form of a factor. As mentioned earlier, this article examined the research and attitudes that had the most in common. Some projects interact with defined protocols and use them, while others offer solutions for integrating protocols. On the other hand, in order to have reliable interoperability between different and smart objects and devices, the issue of standardisation arises [19]. As stated, [41] the Internet of Things always needs standards to interact between new software and hardware. Hence, security protocols play a key role in the future of IoT. As mentioned in the literature review section, the definition of network protocols and standards in specific and limited institutions are determined and explained according to specific criteria.

According to [30] accentuated the importance of the standardisation challenge. They acknowledged that if the challenges of standardisation and protocol are not managed, they will have very irreparable consequences. According to the studies have done in this article, two factors of wireless protocols, data standards from the research [43] can be considered as features of the protocol and standardisation factor. Finally, it should not be added that it is not so that some of the challenges of the Internet of Things are important and some are of lower priority. If only one part of IoT encounters a problem, infiltration may occur from that area.

The sixth and critical factor of IoT included in the key challenges model of this research is energy consumption. The share of energy consumption only through electronic and active devices in IoT has become a very serious and important issue today. Studies show that the use of clean energy has started in smart cities, but there is a lot of work to be done. For example, it should be added that one of the most practical uses of solar energy in the smart city has been in the lighting context. The other article [21] has well pointed out that new devices in the Internet of Things are being produced and used more efficiently day by day. Moreover, one of the most common ways to reduce energy consumption in IoT is its control and management. For instance, cameras and sensors that see a moving object are activated and monitor events. Hence, smart energy is a term that plays a key role in the dynamics and formation of the smart city [32]. This study also examined four features of energy harvesting, energy conservation, energy usage, energy sustainability for the energy consumption factor. Description on saving energy was given above. The Internet of Things vision shows that over time, devices on the Internet will appear to be more efficient. However, the main concern and challenge of this research in this particular case is that the IoT vision is based on expansion and development in various industries. Although the energy consumption of devices will decrease over time, the increasing expansion of IoT in various industries will pose new challenges. Finally, this article believes that for energy conservation as well as sustainability, scientific and academic environments can increase productivity by having practical experience of the Internet of Things services.

Finally, this study believes that have examined those articles and scientific materials that had the most overlap. Based on previous literature and findings, as written in this section, these six key IoT challenges are addressed one after the other and are interdependent.

IV. CONCLUSION

Since the Internet of Things have entered many areas, including industry, agriculture, health, business, and even everyday life, and has linked all of these areas to individuals, it indicates a very large extent. The scope of IoT and the objects and components that are added to it increase every day. Therefore, there will be many challenges in the future and these challenges should be discovered and identified in order to provide solutions for them as soon as possible.

Obviously, the purpose of IoT is to improve the quality of life and reduce the cost of living, and ignoring its challenges will lead to more traffic loads and costs, which endanger the Internet of Things framework. As the Internet of Things grows, so do its challenges. Therefore, six basic factors along with a number of sub-factors were identified and introduced in this article leading to the Internet of Things challenges. The extracted challenges in this article are prepared in the form of Table 1. In this section, we explain these factors overlap with each other.

Table.1. This table indicates the critical challenges mentioned in this research and its most important Sub-Challenges or features.

Main Challenges	**Sub-Challenges or Features**
Security [4] [26] [28] [34] [35] [38] [39] [41] [42][47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [96] [97] [98] [99] [100] [101] [102] [103] [104] [105] [106] [107] [108] [109] [110] [111] [112] [113] [114] [115] [116] [117] [118] [119] [120] [121] [122] [123] [124] [125] & Privacy [15] [21] [24] [28] [34] [38] [41] [50] [55] [62] [64] [70] [71] [75] [94] [98] [103] [115] [120] [121] [126]	Access Control [19] [22] [26] [37] [39] [44] Trust [15] [19] [26] [37] [45] [46] Identification & Authentication [19] [22] [26] [37] [38] [39] Integrity [26] [37] [38] Confidentiality [19] [37] [38] [39] Availability [38] [39]
Scalability [19] [23] [28] [29] [32] [41] [55] [125] [142] [143] [144]	Business [29] [33] [37] [127] [128] [129] [130] Marketing [11] [29] Software [29] [131] [132] [133] Hardware [29] [134] [135] [136] Networks [29] [41] [137] [138] [139] [140] [141]
Interoperability [19] [21] [22] [23] [24] [27] [39] [41] [55] [94] [95] [120] [123] [142]	Virtual Representation of Things [27] [41] Searching, Finding and Accessing Thing [41] [145] Syntactic Interoperability between Thing [41] IPv6 Addressing [19] [38] [40] [42]
Mobility [15] [19] [26] [27] [38] [42] [55] [86] [93] [94] [95] [142]	Detection of Movement of the Device [41] Control Messages [42] [146] Movement Detection [19] [147] [148]
Protocol & Standardisation [19] [28] [29] [30] [41] [43] [117]	Wireless Protocols [30] [43] [149] Data Standards [30] [43] [150]
Energy Consumption [19] [21] [24] [26] [28] [29] [32] [41] [95] [96] [98] [120]	Energy Harvesting [24] [32] [96] [151] [152] [153] [154] Energy Conservation [21] [32] [96] [155] Energy Usage [32] [96] [156] Energy Sustainability [24] [96] [157]

The most critical and key challenges of the Internet of Things in this article is the security and privacy, given the number of citations, because at the risk of it, a large gateway for attacks, vulnerabilities and capital may occur. Because there are millions of IoT-connected devices, the vulnerabilities in the devices that connect to individuals provide easy access for hackers and can be a threshold for advanced attacks.

The Internet of Things assets are all components, objects and devices that are connected to the Internet of Things and they are an important component that loses its popularity among individuals when these assets are endangered.

As mentioned, IoT is a combination of different objects, and according to this article, each has its own security requirements that must be met. In addition to security, the privacy of those involved with these objects is very important so that their personal information is not disclosed. Thus, access control, trust, authentication, integrity, confidentiality and accessibility, if not followed, will destroy the foundations of security. In the absence of security, the Internet of Things objects become zombies that devour individuals. Therefore, with the said materials, there is more focus on the challenges of security and privacy in the world, and there have been many studies emphasising that solutions and techniques should be developed to solve these problems.

By putting together, the achieved challenges, it has made it possible for future researchers to know the challenges of each dimension in IoT, to be able to provide basic and problem-free solutions. This article also argues that all of the above challenges should be controlled and managed in parallel because if one factor is damaged, other factors are also at risk.

As mentioned before, security and privacy are two closely related concepts in the Internet of Things that are discussed in one field in this research. According to the studies conducted, security plays a key role in all levels of the Internet of Things, such as hardware and software. Also, among the 155 articles reviewed, the most focus is on security and privacy. As mentioned in [158], the reason for this importance is the increasing data and information in the network platform as well as the expansion of the network world. Furthermore, conditions including climate diversity, infrastructure, different platforms for diverse projects, and many others have also made it difficult to address the issue of security and privacy. Hence the sub-factors extracted for this field include Access Control, Trust, Identification & Authentication, Integrity, Confidentiality, and Availability. Access control focuses on process-based access management, and trust refers to object authentication and data security, as emphasised in previous studies. As mentioned before, the main and secondary factors in this research are complementary. Therefore, Identification & Authentication is one of the most vulnerable sub-factors and if the identification and authentication is not done securely and as soon as possible, it can endanger the security and privacy of users' information. In this research, the selected factors and sub-factors are complementary to each other, and therefore the Integrity sub-factor after the mentioned sub-factors examines the integrity and ensuring the completeness of the data. The data is then checked through the Confidentiality sub-factor to see if the information reaches the destination with complete accuracy, and finally Availability is the last sub-factor that has been extracted for this study. Availability is a key factor in the Internet of Things, which provides the reliability of users' products in the cloud services.

The second factor investigated and extracted in this study is Scalability. Therefore, the challenges of this factor are always increasing in proportion to the development of the Internet of Things, and its sub-factors include the topics of Business, Marketing, Software, Hardware, Networks.

The third key factor extracted from the 155 articles studied is the Interoperability, systems and platforms in the IoT platform are not of a particular type, and this is exactly the factor that provides communication and sharing among different IoT devices.

Virtual Representation of Things, Searching, Finding and Accessing Thing, Syntactic Interoperability between Thing, IPv6 Addressing were selected as sub-factors of this important issue. As can be seen from the meanings of these sub-factors, access to objects, search, virtual display of objects, interoperability between objects and IPv6 addressing speed up and improve the interoperability of the Internet of Things. However, Mobility has always been one of the most important IoT factors and has been considered as the next factor in this study. According to the results of this research, Mobility indicates productivity and increase in profitability, and companies should also trust this factor in big data analysis. Mobility detection, message control and device mobility detection are the responsibility of the Mobility sub-factors, which may have challenges in wide range.

Protocol & Standardisation is considered as the fifth main factor of this study. Standardisation and definition of protocols in the network world has always been considered in organisations such as IEEE. This includes high levels of security, privacy, integrity, and other factors because everywhere a specific standard and rules are followed, such as data standards and wireless networking protocols, and so on. For example: (Protocol - IEEE 802.11). Energy Consumption is the last key field in this study. Today, energy consumption is one of the main challenges of the Internet of Things. According to studies, network hardware and equipment consume high energy and consequently create warming for the planet. Although some companies have thought of arrangements for this issue, it must be boldly said that this factor is one of the overlooked options in the field of IoT that has not been seriously considered. The sub-factors of this key factor also refer to the amount of used energy, energy saving, energy sustainability, and how to use this energy. As mentioned, this study does not intend to give an overview of this issue, but rather to give an overview to future researchers.

Finally, the six factors and the sub factors have been presented in this article as critical and key challenges based on the explanations given to each and their degree of importance and that they are common to all areas of the Internet of Things.

ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to Dr. Kambiz Partazian and Alireza Rastegariara for their constructive guidance, encouragement and advice.

FUNDING

The author(s) received no financial support for the research, authorship, and/or publication of this article.

CONFLICT OF INTEREST

The authors have no potential conflicts of interest relevant to this article.

REFERENCES

[1] M. I. Pramanik, R. Y. Lau, H. Demirkan, and M. A. K. J. E. S. w. A. Azad, "Smart health: Big data enabled health paradigm within smart cities," vol. 87, pp. 370-383, 2017.

[2] J. Gómez, J. F. Huete, O. Hoyos, L. Perez, and D. J. P. C. S. Grigori, "Interaction system based on internet of things as support for education," vol. 21, pp. 132-139, 2013.

[3] Z. Jun, D. Simplot-Ryl, C. Bisdikian, and H. J. I. C. M. Mouftah, "The internet of things," vol. 49, no. 11, pp. 30-31, 2011.

[4] D. Miorandi, S. Sicari, F. De Pellegrini, and I. J. A. h. n. Chlamtac, "Internet of things: Vision, applications and research challenges," vol. 10, no. 7, pp. 1497-1516, 2012.

[5] J. J. P. Tsitsiklis, Massachusetts Institute of Technology, "Problems in decentralized decision making and computation (1984)."

[6] A. U. J. W. H. O. R. Truth, "No health without a workforce," pp. 1-104, 2013.

[7] B. Rodić-Trmčić, A. Labus, Z. Bogdanović, D. D. Babić, A. J. M. J. o. S. B. Dacić-Pilčević, and M. S. i. E. Economies, "Usability of m-Health services: a health professional's perspective," vol. 21, no. 80, pp. 45-54, 2017.

[8] B. Rodić-Trmčić, A. Labus, D. Barać, S. Popović, and B. J. C. A. i. E. E. Radenković, "Designing a course for smart healthcare engineering education," vol. 26, no. 3, pp. 484-499, 2018.

[9] https://www.smartcity.press/smart-healthcare-for-smart-cities, (August 5, 2017).

[10] R. Pirmagomedov and Y. J. I. o. T. Koucheryavy, "IoT technologies for Augmented Human: A survey," p. 100120, 2019.

[11] F.-Y. Lo, N. J. T. F. Campos, and S. Change, "Blending Internet-of-Things (IoT) solutions into relationship marketing strategies," vol. 137, pp. 10-18, 2018.

[12] C. A. Tokognon, B. Gao, G. Y. Tian, and Y. J. I. I. o. T. J. Yan, "Structural health monitoring framework based on Internet of Things: A survey," vol. 4, no. 3, pp. 619-635, 2017.

[13] G. Reggio, M. Leotta, M. Cerioli, R. Spalazzese, and F. J. I. o. T. Alkhabbas, "What Are IoT Systems for Real? An Experts' Survey on Software Engineering Aspects," p. 100313, 2020.

[14] M. Otoom, N. Otoum, M. A. Alzubaidi, Y. Etoom, R. J. B. S. P. Banihani, and Control, "An IoT-based framework for early identification and monitoring of COVID-19 cases," vol. 62, p. 102149, 2020.

[15] F. Lotfi and A. Soleimani, "A Model to Stabilize E-Loyalty to Healthcare Services in the Context of the Internet of Things by using Fuzzy AHP Method," in 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2020, pp. 8-13: IEEE.

[16] V. R. Kebande, P. P. Mudau, R. A. Ikuesan, H. Venter, and K.-K. R. J. F. S. I. R. Choo, "Holistic digital forensic readiness framework for IoT-enabled organizations," vol. 2, p. 100117, 2020.

[17] F. Cauteruccio et al., "A framework for anomaly detection and classification in Multiple IoT scenarios," vol. 114, pp. 322-335, 2020.

[18] M. Nobakht, C. Russell, W. Hu, and A. Seneviratne, "IoT-NetSec: policy-based IoT network security using OpenFlow," in 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 955-960: IEEE.

[19] A. Triantafyllou, P. Sarigiannidis, T. D. J. W. c. Lagkas, and m. computing, "Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends," vol. 2018, 2018.

[20] H. Ning, H. Liu, and L. T. J. C. Yang, "Cyberentity security in the internet of things," vol. 46, no. 4, pp. 46-53, 2013.

[21] S. Kumar, P. Tiwari, and M. J. J. o. B. D. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," vol. 6, no. 1, p. 111, 2019.

[22] M. Noura, M. Atiquzzaman, M. J. M. N. Gaedke, and Applications, "Interoperability in internet of things: Taxonomies and open challenges," vol. 24, no. 3, pp. 796-809, 2019.

[23] R. Mijumbi et al., "Network function virtualization: State-of-the-art and research challenges," vol. 18, no. 1, pp. 236-262, 2015.

[24] S. Chen, H. Xu, D. Liu, B. Hu, and H. J. I. I. o. T. j. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," vol. 1, no. 4, pp. 349-359, 2014.

[25] https://smarttampere.fi/en/network/smart-mobility/, 2020.

[26] S. Sicari, A. Rizzardi, L. A. Grieco, and A. J. C. n. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," vol. 76, pp. 146-164, 2015.

[27] L. Bittencourt et al., "The internet of things, fog and cloud continuum: Integration and challenges," vol. 3, pp. 134-155, 2018.

[28] M. Thibaud, H. Chi, W. Zhou, and S. J. D. S. S. Piramuthu, "Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review," vol. 108, pp. 79-95, 2018.

[29] A. Gupta, R. Christie, and P. J. I. J. C. I. R. Manjula, "Scalability in internet of things: features, techniques and research challenges," vol. 13, no. 7, pp. 1617-1627, 2017.

[30] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," in 2016 Future Technologies Conference (FTC), 2016, pp. 731-738: IEEE.

[31] https://news.microsoft.com/features/under-the-sea-microsoft-tests-a-datacenter-thats-quick-to-deploy-could-provide-internet-connectivity-for-years/.

[32] R. van Kranenburg and A. Bassi, "IoT Challenges," Communications in Mobile Computing, vol. 1, no. 1, p. 9, 2012/11/28 2012.

[33] F. Lotfi, K. Fatehi, and N. Badie, "An Analysis of Key Factors to Mobile Health Adoption using Fuzzy AHP."

[34] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. J. I. j. o. c. a. Kamal, "A review on internet of things (IoT)," vol. 113, no. 1, pp. 1-7, 2015.

[35] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 2012, vol. 3, pp. 1062-1066: IEEE.

[36] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. J. W. N. Qiu, "Security of the Internet of Things: perspectives and challenges," vol. 20, no. 8, pp. 2481-2501, 2014.

[37] R. Roman, J. Zhou, and J. J. C. N. Lopez, "On the features and challenges of security and privacy in distributed internet of things," vol. 57, no. 10, pp. 2266-2279, 2013.

[38] A. J. Jara, L. Ladid, and A. F. J. J. W. M. N. U. C. D. A. Gómez-Skarmeta, "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities," vol. 4, no. 3, pp. 97-118, 2013.

[39] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. J. I. I. o. T. J. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," vol. 4, no. 5, pp. 1125-1142, 2017.

[40] T. Savolainen, J. Soininen, and B. J. I. S. J. Silverajan, "IPv6 addressing strategies for IoT," vol. 13, no. 10, pp. 3511-3519, 2013.

[41] M. Elkhodr, S. Shahrestani, and H. J. a. p. a. Cheung, "The internet of things: new interoperability, management and security challenges," 2016.

[42] Q. Emad-ul-Haq et al., "Challenges and solutions for Internet of Things Driven by IPv6," vol. 9, no. 12, 2015.

[43] T. Vresk and I. Čavrak, "Architecture of an interoperable IoT platform based on microservices," in 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016, pp. 1196-1201: IEEE.

[44] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," Mathematical and Computer Modelling, vol. 58, no. 5, pp. 1189-1205, 2013/09/01/ 2013.

[45] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security," Journal of Information Security and Applications, vol. 52, p. 102467, 2020/06/01/ 2020.

[46] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," Future Generation Computer Systems, vol. 108, pp. 909-920, 2020/07/01/ 2020.

[47] Y. Xie and D. Wang, "An item-level access control framework for inter-system security in the internet of things," in Applied mechanics and materials, 2014, vol. 548, pp. 1430-1432: Trans Tech Publ.

[48] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2014, pp. 165-172: IEEE.

[49] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited connections: a study of vulnerable devices on the internet of things (IoT)," in 2014 IEEE Joint Intelligence and Security Informatics Conference, 2014, pp. 232-235: IEEE.

[50] R. H. J. C. l. Weber and s. review, "Internet of Things–New security and privacy challenges," vol. 26, no. 1, pp. 23-30, 2010.

[51] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, "Identity management framework towards internet of things (IoT): Roadmap and key challenges," in International Conference on Network Security and Applications, 2010, pp. 430-439: Springer.

[52] H. Yi and Z. J. F. G. C. S. Nie, "Side-channel security analysis of UOV signature for cloud-based Internet of Things," vol. 86, pp. 704-708, 2018.

[53] A. R. Sfar, Z. Chtourou, and Y. Challal, "A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges," in 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C), 2017, pp. 101-105: IEEE.

[54] K. Gatsis and G. J. Pappas, "Wireless control for the iot: Power, spectrum, and security challenges," in 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), 2017, pp. 341-342: IEEE.

[55] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," in 2016 IEEE Smart Energy Grid Engineering (SEGE), 2016, pp. 381-385: IEEE.

[56] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)," in 2017 Eleventh International Conference on Sensing Technology (ICST), 2017, pp. 1-5: IEEE.

[57] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. J. I. I. o. T. J. Sheng, "IoT middleware: A survey on issues and enabling technologies," vol. 4, no. 1, pp. 1-20, 2016.

[58] A. Mosenia and N. K. J. I. T. o. E. T. i. C. Jha, "A comprehensive study of security of internet-of-things," vol. 5, no. 4, pp. 586-602, 2016.

[59] Y. Yang, L. Wu, G. Yin, L. Li, and H. J. I. I. o. T. J. Zhao, "A survey on security and privacy issues in Internet-of-Things," vol. 4, no. 5, pp. 1250-1258, 2017.

[60] P. I. R. Grammatikis, P. G. Sarigiannidis, and I. D. J. I. o. T. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," vol. 5, pp. 41-70, 2019.

[61] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5772-5781: IEEE.

[62] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. J. I. i. o. t. j. Xu, "Edge computing: Vision and challenges," vol. 3, no. 5, pp. 637-646, 2016.

[63] X. Liu, Y. Yang, K.-K. R. Choo, H. J. W. C. Wang, and M. Computing, "Security and privacy challenges for Internet-of-Things and fog computing," vol. 2018, 2018.

[64] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities," in

2014 IEEE 7th international conference on service-oriented computing and applications, 2014, pp. 230-234: IEEE.

[65] A. K. Mohammadzadeh, S. Ghafoori, A. Mohammadian, R. Mohammadkazemi, B. Mahbanooei, and R. J. T. i. S. Ghasemi, "A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran," vol. 53, pp. 124-134, 2018.

[66] M. B. Mollah, M. A. K. Azad, A. J. J. o. N. Vasilakos, and C. Applications, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," vol. 84, pp. 38-54, 2017.

[67] F. A. Alaba, M. Othman, I. A. T. Hashem, F. J. J. o. N. Alotaibi, and C. Applications, "Internet of Things security: A survey," vol. 88, pp. 10-28, 2017.

[68] P. Schaumont, "Security in the Internet of Things: A challenge of scale," in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017, 2017, pp. 674-679: IEEE.

[69] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 180-187: IEEE.

[70] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. A. J. C. N. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," vol. 112, pp. 237-262, 2017.

[71] M. Sain, Y. J. Kang, and H. J. Lee, "Survey on security in Internet of Things: State of the art and challenges," in 2017 19th International conference on advanced communication technology (ICACT), 2017, pp. 699-704: IEEE.

[72] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 336-341: IEEE.

[73] X. Xiaohui, "Study on security problems and key technologies of the internet of things," in 2013 International conference on computational and information sciences, 2013, pp. 407-410: IEEE.

[74] L. M. Dang, M. Piran, D. Han, K. Min, and H. J. E. Moon, "A survey on internet of things and cloud computing for healthcare," vol. 8, no. 7, p. 768, 2019.

[75] A. R. Sfar, E. Natalizio, Y. Challal, Z. J. D. C. Chtourou, and Networks, "A roadmap for security challenges in the Internet of Things," vol. 4, no. 2, pp. 118-137, 2018.

[76] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," in Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, 2015, pp. 37-42.

[77] A. K. Das, S. Zeadally, and D. J. F. G. C. S. He, "Taxonomy and analysis of security protocols for Internet of Things," vol. 89, pp. 110-125, 2018.

[78] B. Di Martino, M. Rak, M. Ficco, A. Esposito, S. A. Maisto, and S. J. I. o. T. Nacchia, "Internet of things reference architectures, security and interoperability: A survey," vol. 1, pp. 99-112, 2018.

[79] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. J. I. A. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," vol. 7, pp. 82721-82743, 2019.

[80] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "IoT based smart security and home automation system," in 2016 international conference on computing, communication and automation (ICCCA), 2016, pp. 1286-1289: IEEE.

[81] X. C. Yin, Z. G. Liu, L. Nkenyereye, and B. J. S. Ndibanje, "Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach," vol. 19, no. 22, p. 4952, 2019.

[82] B. Xu et al., "A security design for the detecting of buffer overflow attacks in iot device," vol. 6, pp. 72862-72869, 2018.

[83] I. Kotenko, I. Saenko, and A. J. I. A. Branitskiy, "Framework for mobile Internet of Things security monitoring based on big data processing and machine learning," vol. 6, pp. 72714-72723, 2018.

[84] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. J. I. A. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," vol. 7, pp. 13960-13988, 2019.

[85] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. J. W. P. C. Wehrle, "Security Challenges in the IP-based Internet of Things," vol. 61, no. 3, pp. 527-542, 2011.

[86] P. Ray, "A survey on internet of things architectures. J King of Saud Univ Comput Inf Sci," ed: Elsevier, 2018.

[87] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. J. I. C. S. Faruki, and Tutorials, "Network intrusion detection for IoT security based on learning techniques," vol. 21, no. 3, pp. 2671-2701, 2019.

[88] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. J. I. I. o. T. J. Burnap, "A supervised intrusion detection system for smart home IoT devices," vol. 6, no. 5, pp. 9042-9053, 2019.

[89] N. Wang, T. Jiang, S. Lv, and L. J. I. C. L. Xiao, "Physical-layer authentication based on extreme learning machine," vol. 21, no. 7, pp. 1557-1560, 2017.

[90] L. Wei, W. Luo, J. Weng, Y. Zhong, X. Zhang, and Z. J. I. A. Yan, "Machine learning-based malicious application detection of android," vol. 5, pp. 25591-25601, 2017.

[91] D. Mocrii, Y. Chen, and P. J. I. o. T. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," vol. 1, pp. 81-98, 2018.

[92] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in 2012 international conference on computer science and electronics engineering, 2012, vol. 3, pp. 648-651: IEEE.

[93] H. Sundmaeker, P. Guillemin, P. Friess, and S. J. C. o. E. R. P. o. t. I. o. T. Woelfflé, European Commision, "Vision and challenges for realising the Internet of Things," vol. 3, no. 3, pp. 34-36, 2010.

[94] A. A. G.-E. Ahmed, "Benefits and Challenges of Internet of Things for Telecommunication Networks," in Telecommunication Networks-Trends and Developments: IntechOpen, 2019.

[95] T. Salman and R. J. a. p. a. Jain, "A survey of protocols and standards for internet of things," 2019.

[96] H. Lee, "The internet of things and assistive technologies for people with disabilities: Applications, trends, and issues," in Internet of things and advanced application in healthcare: IGI Global, 2017, pp. 32-65.

[97] H. Madsen, B. Burtschy, G. Albeanu, and F. Popentiu-Vladicescu, "Reliability in the utility computing era: Towards reliable fog computing," in 2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP), 2013, pp. 43-46: IEEE.

[98] M. Chiang and T. J. I. I. o. T. J. Zhang, "Fog and IoT: An overview of research opportunities," vol. 3, no. 6, pp. 854-864, 2016.

[99] S. S. Gill et al., "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges," vol. 8, p. 100118, 2019.

[100] D. S. Kim, T.-H. Shin, B. Lee, and J. S. Park, "Access control and authorization for security of RFID multi-domain using SAML and XACML," in International Conference on Computational and Information Science, 2006, pp. 887-893: Springer.

[101] A. Dehghantanha and K. Franke, "Privacy-respecting digital investigation," in 2014 Twelfth Annual International Conference on Privacy, Security and Trust, 2014, pp. 129-138: IEEE.

[102] W. Wei, A. T. Yang, W. Shi, and K. Sha, "Security in internet of things: Opportunities and challenges," in 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), 2016, pp. 512-518: IEEE.

[103] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, and M. J. I. C. M. Mohammadi, "Toward better horizontal integration among IoT services," vol. 53, no. 9, pp. 72-79, 2015.

[104] D. Chasaki, C. J. I. J. o. S.-B. Mansour, and S. Computing, "Security challenges in the internet of things," vol. 5, no. 3, pp. 141-149, 2015.

[105] J. M. McGinthy, L. J. Wong, and A. J. J. I. I. o. T. J. Michaels, "Groundwork for neural network-based specific emitter identification authentication for IoT," vol. 6, no. 4, pp. 6429-6440, 2019.

[106] N. M. Kumar and P. K. J. P. C. S. Mallick, "Blockchain technology for security issues and challenges in IoT," vol. 132, pp. 1815-1823, 2018.

[107] K. M. Sadique, R. Rahmani, and P. J. P. C. S. Johannesson, "Towards security on internet of things: applications and challenges in technology," vol. 141, pp. 199-206, 2018.

[108] K. Zhu, Z. Chen, W. Yan, and L. J. I. I. o. T. J. Zhang, "Security attacks in named data networking of things and a blockchain solution," vol. 6, no. 3, pp. 4733-4741, 2018.

[109] G. Gan, Z. Lu, and J. Jiang, "Internet of things security analysis," in 2011 international conference on internet technology and applications, 2011, pp. 1-4: IEEE.

[110] K. Zhao and L. Ge, "A survey on the internet of things security," in 2013 Ninth international conference on computational intelligence and security, 2013, pp. 663-667: IEEE.

[111] B. K. Mohanta, U. Satapathy, S. S. Panda, and D. Jena, "A Novel Approach to Solve Security and Privacy Issues for IoT Applications Using Blockchain," in 2019 International Conference on Information Technology (ICIT), 2019, pp. 394-399: IEEE.

[112] B. K. Mohanta, D. Jena, U. Satapathy, and S. J. I. o. T. Patnaik, "Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology," p. 100227, 2020.

[113] A. Dorri, C. Roulin, R. Jurdak, and S. S. Kanhere, "On the activity privacy of blockchain for IoT," in 2019 IEEE 44th Conference on Local Computer Networks (LCN), 2019, pp. 258-261: IEEE.

[114] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. J. I. T. o. I. I. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," vol. 15, no. 6, pp. 3680-3689, 2019.

[115] A. Čolaković and M. J. C. N. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," vol. 144, pp. 17-39, 2018.

[116] E. J. J. o. C. Leloglu and Communications, "A review of security concerns in Internet of Things," vol. 5, no. 1, pp. 121-136, 2016.

[117] J. Granjal, E. Monteiro, J. S. J. I. C. S. Silva, and Tutorials, "Security for the internet of things: a survey of existing protocols and open research issues," vol. 17, no. 3, pp. 1294-1312, 2015.

[118] M. B. Line, I. A. T◌̋ndel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in 2011 2nd IEEE PES international conference and exhibition on innovative smart grid technologies, 2011, pp. 1-8: IEEE.

[119] B. Afzal, M. Umair, G. A. Shah, and E. J. F. G. C. S. Ahmed, "Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges," vol. 92, pp. 718-731, 2019.

[120] K. J. I. J. o. E. S. Patel and Computing, "K. & Patel, S., M. 2016. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," vol. 6, no. 5.

[121] I. Lee and K. J. B. H. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," vol. 58, no. 4, pp. 431-440, 2015.

[122] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. J. I. o. T. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," p. 100129, 2019.

[123] E. G. Petrakis, S. Sotiriadis, T. Soultanopoulos, P. T. Renta, R. Buyya, and N. J. I. o. T. Bessis, "Internet of Things as a Service (iTaaS): Challenges and Solutions for Management of Sensor Data on the Cloud and the Fog," vol. 3, pp. 156-174, 2018.

[124] M. Tavana, V. Hajipour, and S. J. I. o. T. Oveisi, "IoT-based Enterprise Resource Planning: Challenges, Open Issues, Applications, Architecture, and Future Research Directions," p. 100262, 2020.

[125] S. Floriano, "Market challenges of incumbent telecom companies entering Internet-of-Things (IoT) ecosystems and organizational implications: A case study," ed, 2018.

[126] C. Esposito, A. Castiglione, C.-A. Tudorica, and F. J. I. C. M. Pop, "Security and privacy for cloud-based data management in the health network service chain: a microservice approach," vol. 55, no. 9, pp. 102-108, 2017.

[127] S. Leminen, M. Rajahonka, R. Wendelin, and M. Westerlund, "Industrial internet of things business models in the machine-to-machine context," Industrial Marketing Management, vol. 84, pp. 298-311, 2020/01/01/ 2020.

[128] M. Palmaccio, G. Dicuonzo, and Z. S. Belyaeva, "The internet of things and corporate business models: A systematic literature review," Journal of Business Research, 2020/10/10/ 2020.

[129] A. Sestino, M. I. Prete, L. Piper, and G. Guido, "Internet of Things and Big Data as enablers for business digitalization strategies," Technovation, vol. 98, p. 102173, 2020/12/01/ 2020.

[130] D. J. Langley, J. van Doorn, I. C. L. Ng, S. Stieglitz, A. Lazovik, and A. Boonstra, "The Internet of Everything: Smart things and their impact on business models," Journal of Business Research, vol. 122, pp. 853-863, 2021/01/01/ 2021.

[131] G. Reggio, M. Leotta, M. Cerioli, R. Spalazzese, and F. Alkhabbas, "What are IoT systems for real? An experts' survey on software engineering aspects," Internet of Things, vol. 12, p. 100313, 2020/12/01/ 2020.

[132] W. Niu, X. Zhang, X. Du, L. Zhao, R. Cao, and M. Guizani, "A deep learning based static taint analysis approach for IoT software vulnerability location," Measurement, vol. 152, p. 107139, 2020/02/01/ 2020.

[133] S. Traboulsi and S. Knauth, "Towards implementation of an IoT analysis system for buildings environmental data and workplace well-being with an IoT open software," Procedia Computer Science, vol. 170, pp. 341-346, 2020/01/01/ 2020.

[134] M. Suresh and M. Neema, "Hardware Implementation of Blowfish Algorithm for the Secure Data Transmission in Internet of Things," Procedia Technology, vol. 25, pp. 248-255, 2016/01/01/ 2016.

[135] A. Burger, C. Cichiwskyj, S. Schmeiكer, and G. Schiele, "The Elastic Internet of Things - A platform for self-integrating and self-adaptive IoT-systems with support for embedded adaptive hardware," Future Generation Computer Systems, vol. 113, pp. 607-619, 2020/12/01/ 2020.

[136] T. Jung, N. Jazdi, S. Krauك, C. K◌ِllner, and M. Weyrich, "Hardware-in-the-Loop Simulation for a Dynamic Co-Simulation of Internet-of-Things-Components," Procedia CIRP, vol. 93, pp. 1334-1339, 2020/01/01/ 2020.

[137] Q. Guo and Q. Xu, "nThe Economic Benefits of Agglomeration of The Internet of Things Industry Based on 5G Network and Markov Chain," Microprocessors and Microsystems, p. 103438, 2020/11/09/ 2020.

[138] K. Zhan, "Sports and health big data system based on 5G network and Internet of Things system," Microprocessors and Microsystems, p. 103363, 2020/11/01/ 2020.

[139] K. Cheng, "Smart Rural Financial Innovation based on 5G Network and Internet of Things," Microprocessors and Microsystems, p. 103500, 2020/11/18/ 2020.

[140] M. Wang and Q. Yang, "Green building design based on 5G network and Internet of Things system," Microprocessors and Microsystems, p. 103386, 2020/11/06/ 2020.

[141] H. Bai and Q. Zhang, "English smart classroom teaching system based on 5 network and internet of things," Microprocessors and Microsystems, p. 103421, 2020/11/08/ 2020.

[142] A. Khanna and S. Kaur, "Internet of Things (IoT), Applications and Challenges: A Comprehensive Review."

[143] H. Vahdat-Nejad, Z. Mazhar-Farimani, and A. Tavakolifar, "Social Internet of Things and New Generation Computing—A Survey," in Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications: Springer, 2020, pp. 139-149.

[144] R. Van Kranenburg and A. J. C. i. M. C. Bassi, "IoT challenges," vol. 1, no. 1, p. 9, 2012.

[145] D. Xue, Y. Cheng, and P. Gope, "2 - An efficient ambient intelligent–assisted people searching for Internet of Things–based health-care system," in Assistive Technology for the Elderly, N. K. Suryadevara and S. C. Mukhopadhyay, Eds.: Academic Press, 2020, pp. 45-58.

[146] J. Hua and K. Sakurai, "Botnet command and control based on Short Message Service and human mobility," Computer Networks, vol. 57, no. 2, pp. 579-597, 2013/02/04/ 2013.

[147] M. Bouaziz, A. Rachedi, and A. Belghith, "EKF-MRPL: Advanced mobility support routing protocol for internet of mobile things: Movement prediction approach," Future Generation Computer Systems, vol. 93, pp. 822-832, 2019/04/01/ 2019.

[148] H. Yuan, Y. Qian, R. Yang, and M. Ren, "Human mobility discovering and movement intention detection with GPS trajectories," Decision Support Systems, vol. 63, pp. 39-51, 2014/07/01/ 2014.

[149] A. Roy and N. Sarma, "A synchronous duty-cycled reservation based MAC protocol for underwater wireless sensor networks," Digital Communications and Networks, 2020/09/28/ 2020.

[150] W. Kubick, "Chapter 21 - Re-Engineering Clinical Research with Data Standards," in Re-Engineering Clinical Trials, P. Schüler and B. Buckley, Eds. Boston: Academic Press, 2015, pp. 227-243.

[151] P. Choudhary, L. Bhargava, V. Singh, M. Choudhary, and A. k. Suhag, "A survey – Energy harvesting sources and techniques for internet of things devices," Materials Today: Proceedings, vol. 30, pp. 52-56, 2020/01/01/ 2020.

[152] S. Zeadally, F. K. Shaikh, A. Talpur, and Q. Z. Sheng, "Design architectures for energy harvesting in the Internet of Things," Renewable and Sustainable Energy Reviews, vol. 128, p. 109901, 2020/08/01/ 2020.

[153] T. Tan et al., "Renewable energy harvesting and absorbing via multi-scale metamaterial systems for Internet of things," Applied Energy, vol. 254, p. 113717, 2019/11/15/ 2019.

[154] S. Sadowski and P. Spachos, "Wireless technologies for smart agricultural monitoring using internet of things devices with energy harvesting capabilities," Computers and Electronics in Agriculture, vol. 172, p. 105338, 2020/05/01/ 2020.

[155] A. Perles et al., "An energy-efficient internet of things (IoT) architecture for preventive conservation of cultural heritage," Future Generation Computer Systems, vol. 81, pp. 566-581, 2018/04/01/ 2018.

[156] H. N. Rafsanjani and A. Ghahramani, "Towards utilizing internet of things (IoT) devices for understanding individual occupants' energy usage of personal and shared appliances in office buildings," Journal of Building Engineering, vol. 27, p. 100948, 2020/01/01/ 2020.

[157] P. K. Khatua, V. K. Ramachandaramurthy, P. Kasinathan, J. Y. Yong, J. Pasupuleti, and A. Rajagopalan, "Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues," Sustainable Cities and Society, vol. 53, p. 101957, 2020/02/01/ 2020.

[158] V. Chellappan and K. Sivalingam, "Security and privacy in the Internet of Things," in Internet of Things: Elsevier, 2016, pp. 183-200.